Attachment C

PERFORMANCE WORK STATEMENT (PWS)

Installation Campus Area Network Modernization (ICANMOD) Survey, Engineering, and Implementation (SEI) Support Services 2.0

Product Manager (PdM)

Installation Information Infrastructure Modernization (I3MP)

1.0 INTRODUCTION/BACKGROUND

The US Army's Product Manager Installation Information Infrastructure Modernization Program (PdM I3MP) has an ongoing requirement for network engineering and program management support services that are necessary for the successful engineering, installation, configuration, testing, cut-over, and support of network modernization efforts. These efforts include, but are not limited to engineering and related support services that effectively and efficiently modernize the Installation Campus Area Network (ICAN) infrastructure.

PdM I3MP is currently the primary program for accomplishing information technology modernization for Army and Joint Base/Post/Camps/Stations (B/P/C/S) America's area of responsibilities (NORTHCOM and SOUTHCOM). PdM I3MP enables the Warfighter through information technology, infrastructure modernization, and life cycle management of the Army's Installation Campus Area (Voice, Video & Data) Networks, Strategic and Home Station Mission Command Centers (SCC/HSMCC) and Tech Control Facilities (TCF). PdM I3MP, In Accordance With (IAW) the Department of the Army's approved prioritization lists and through the use of Commercial-Off-The-Shelf (COTS) products and borrowed military manpower (BMM), replaces the antiquated, costly, unsupportable and maintenance intensive legacy systems with an integrated information system that is state-of-the-art, secure, interoperable and capable of passing voice/data/video traffic.

I3MP provides a suite of standardized capabilities used at Army Corps, Division & Theater Headquarters' (HQ)'s and core Command, Control, Communications, Computers and Intelligence (C4I) infrastructure for Joint, Coalition & Interagency capabilities at Army Supported Command Centers. These installation infrastructures and capabilities are capable of supporting national strategic communications capabilities for the Army, Department of Defense (DoD) and the National Command Authority (NCA) to enable information dominance.

Since 2013, PdM I3MP has been modernizing the ICAN for 80+ B/P/C/S across CONUS. ICAN upgrades include new 10GbE Ethernet switches and routers and re-engineered to the latest version of the Defense Information System Network (DISN) ICAN Design and Implementation (ICAN-DI) standards. These upgrades prepared the ICAN for migration to the Defense Information Systems Agency (DISA) Multiprotocol Label Switching (MPLS) Wide Area Network (WAN) and the Joint Regional Security Stacks (JRSS). This effort, NETMOD 1.0 was essentially completed in late 2019.

2.0 OBJECTIVES

The Army must now begin the process of surveying, engineering and implementing a

life cycle refresh of the ICAN infrastructure at designated B/P/C/S with new Ethernet switches and routers leveraging assets from multiple organizations. This ICAN life cycle refresh will continue to be a joint US Army/DISA effort with support and resources provided by PdM I3MP, US Army Cyber Command (ARCYBER), US Army Network Engineering Command (NETCOM), 7th Signal Command (Theater) [7th SC (T)], their supporting Signal Brigades (93rd, 106th, 21st), as well as Network Enterprise Centers (NECs). PdM I3MP will act as the lead system integrator and will orchestrate the efforts of both Contractor, Government, Military and Civilian personnel to accomplish this life cycle refresh. PdM I3MP requires a Contractor capable of working in an environment as a team member with the primary responsibilities of surveying, engineering and leading implementation efforts for this life cycle refresh with support and assistance from other Government and Contractor partners.

3.0 SCOPE OF WORK

The Contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision and other items/services (not including those designated as Government - Furnished Equipment (GFE) that are necessary to perform the tasks as defined in this PWS.

The Contractor shall provide engineering and installation support for the US Army's ICAN modernization project which will be managed by PdM I3MP. The Contractor shall survey, engineer and lead implementation efforts that enhance the existing network, ensure availability of mission applications, troubleshoot, and resolve problems with associated Information Technology (IT) equipment.

The Contractor shall directly support the PdM I3MP, Technical Management Division (TMD), I3MP Project Officers, and the Product Manager.

4.0 PERIOD OF PERFORMANCE

Refer to section F.1 of the TOR.

5.0 PLACE OF PERFORMANCE

The primary place of work shall be the Contractor's facility except when onsite at US Army B/P/C/S identified in Attachment 1, DoD CONUS locations (include tail sites), over the duration of this contract PoP. The United States Government (USG) is not obligated to fund performance at all sites included in the comprehensive list nor are obligated to fund all items identified in the site survey report. The Contractor shall provide workspace and all required supporting office equipment and services, at its own facilities for staff members when not assigned to any B/P/C/S. The Contractor shall

coordinate meetings with I3MP staff at Ft Belvoir, VA as determined by the USG.

To the extent possible, the Contractor shall work with the Government Contracting Officer's Representative (COR) at the start of this contract, and at appropriate intervals, to prioritize tasks within this effort. If the Government reprioritizes the sites, the Contractor shall use its best efforts to provide the same level of support as stated in the PWS. In the event that an increased level of effort is required, only the Contracting Officer (KO) may request a modification or an equitable adjustment pursuant to the changes clause of the contract.

6.0 TYPE OF CONTRACT

The government will award a Firm Fixed Price (FFP) contract with Cost Reimbursable (CR) travel and material CLINs

7.0 REQUIREMENTS

As part of the Network Engineering, Integration, and Implementation Support, the Contractor shall be responsible for providing the following support, described in the subsections below:

7.1 ICAN PROGRAM TECHNICAL MANAGEMENT SERVICES

The objective of this effort is to provide program management and technical management services to the PdM I3MP office, facilitating the completion of B/P/C/S IT modernization upgrades.

7.1.1 PROGRAM MANAGEMENT

The Contractor shall provide Program Management Services to include, but not limited to:

a. Drafting, analyzing, integrating, reviewing, and providing recommendations for program milestones and other documentation in accordance with (IAW) Government, Department of Defense (DoD) and US Army regulations.

b. Recommending resolution of issues for program milestone decisions.

c. Providing input to the PdM I3MP Integrated Master Schedule (IMS), IAW Contractor Data Requirements List (CDRL) A005 master implementation, testing and transition plans IAW the CDRL identified in Table 1 of this PWS. The Contractor shall receive USG approval prior to commencing work at a US Army B/P/C/S.

d. Tracking dependencies from ongoing or future projects such as:

- Outside Plant (OSP) remediation
- Facilities infrastructure remediation (e.g. Heating Ventilation and Air Conditioning (HVAC), power, grounding, Inside Plant (ISP) upgrades, etc.)
- Time Division Multiplexing (TDM) Voice Switch decommissioning
- Building construction and/or renovations
- DISA Multi-Protocol Label Switching (MPLS) upgrades
- DISA Joint Regional Security Stacks (JRSS) implementations
- US Army Data Center Consolidation
- Army Enterprise Voice over IP (VoIP)
- Army Unified Capability Soft Client Subscription Service (UC SCSS)
- Army Enterprise IT as a Service (EITaaS)
- Army Synthetic Training Environment (STE)

e. Establishing a deployment methodology that has up to four project installs occurring in parallel.

f. Developing a Project Management Plan (PMP) IAW CDRL A006, which shall describe how the project will be planned, executed, monitored, controlled and closed. The PMP shall include as a minimum:

- Quality Management Plan (QMP) IAW CDRL A007
- Risk Management Plan (RMP) IAW CDRL A008
- Contractor's Safety/Accident Plan IAW CDRL A010
- Configuration Management Plan (CMP) IAW CDRL A011
- Training Plan for the Prime Contractor and Subcontractors (i.e., compliance with Anti-Terrorism Training, Combating Human Trafficking) IAW CDRL A012
- Operations Security (OPSEC) Plan IAW CDRL A009

g. Preparing and maintaining project documentation.

h. Providing project support for reviews, conferences, briefings and associated meetings.

i. Providing recommendations for planning, organizing, managing critical aspects of the development, production and/or deployment of capabilities.

j. Present Weekly Status Reports IAW CDRL A018 electronically to PdM I3MP Team Leadership; attend and support PdM I3MP Monthly PSR briefings (Briefing Materials) IAW CDRL A004.

k. Prepare, review and evaluate fielding documentation, prior to implementation and project closeout (Technical Acceptance Report) IAW CDRL A013 and review fielding plans and recommend for approval / disapproval. Develop, coordinate and synchronize staff actions with Government matrix, and support contractors responsible for materiel fielding processes. Make recommendations and process improvements.

l. Track GFE (as part of the Inventory Records, Procurement List of Materials (LOM) IAW CDRL A002, receive incoming shipments and assist in deploying stored equipment. Perform quality assurance on asset inventory, resolve logistical operational issues, process and record all asset marked items that are delivered to PdM I3MP with unique item identifiers, encoded in machine-readable symbols that distinguish an item from all other like and unlike items.

m. The Government will provide warehouse space on Ft Belvoir for storing, issuing, receiving a small set of Installation Bill of Materials (IBOM) i.e. patch cords, hand trucks, etc. to fill shortages/emergency needs during deployment. Tobyhanna Army Depot (TYAD) shall purchase, store, maintain inventories and distribute most IBOM material. The Contractor shall coordinate with I3MP and TYAD personnel to ensure IBOM material is ordered in time for implementation at each B/P/C/S. The Government shall procure Major Bill of Material (MBOM), IAW CDRL A014 i.e. Ethernet switches, routers, optics, supporting software, etc. though separate contracts provided to the contractor as GFE. The Government shall use the Defense Logistics Agency (DLA) or GFE vendor for storing, inventorying and issuing MBOM equipment for each B/P/C/S. The Contractor shall coordinate with I3MP for MBOM quantities required based on survey results in sufficient time for procurement lead times.

n. Create, update, and maintain MS Project Integrated Master Schedule (IMS) content for PdM I3MP projects. Each program activity will be able to deposit and

maintain all related engineering documents, schedules, briefings and program related materials for ease of access and accountability.

7.1.2 TECHNICAL SUPPORT SERVICES

The Contractor shall provide technical support services. These activities shall include, but are not limited to:

a. Providing site-specific technical guidance and methodologies to implement the new network infrastructure on the B/P/C/S ICAN.

b. Acting as the technical liaison between US Army PdM I3MP Team, 7th Signal Command (Theater) (7th SC(T)), 93rd Signal Brigade (SB), 21st SB, 106th SB, and the Network Enterprise Centers (NECs).

c. Support for I3MP Network Project Team.

d. Providing senior network modernization ACS/ADS/EAS engineering resources to develop and maintain a cohesive engineering approach for the recommended installation activities for each designated B/P/C/S. The Contractor shall provide the Subject Matter Experts (SME) to support generation of Tactics, Techniques and Procedures (TTP).

e. Providing engineering resources to perform technical analysis, trade-off studies, risk assessment and mitigations, Courses of Action (COA) recommendations, briefing presentations, etc. to USG regarding networks survey, engineering, and implementation.

f. Provide exclusive lab environment in Contractor facilities to support any and all required testing for Army approved hardware and operating system revisions that will be deployed in support of the network modernization. Access to the contractor lab for Government staff will be coordinated.

g. Technical engineering support that is experienced with supporting site installations using 802.1X, Network Access Control (NAC), wireless technology, VoIP UC systems, Land Mobile Radio (LMR), etc., as it relates to the implementation and cutover to new hardware.

7.1.3 PRE-SITE SURVEY ACTIVITIES

The Contractor shall collaborate with the Government for the purpose of ensuring the completeness of the following action items before the survey activities take place:

a. The Contractor shall collaborate with the Government for the purpose to facilitate a Kick-Off Meeting (KOM) with each site listed in PWS DoD CONUS locations (Attachment 1), 30 days prior to survey, at which time remote network access will be requested.

b. The B/P/C/S will complete the pre-survey artifact 2 checklist.

c. Remote network access will be made available to the Contractor no later than 20 days prior to survey.

d. Automated network survey results will be greater than 90 percent complete prior to the survey date.

e. The NEC will supply hostname information prior to EIP Version 2.

f. Travel Authorization Requests will be approved at least ten days prior to survey travel date.

g. The Contractor shall collaborate with the Government to discuss all of the Original Equipment Manufacturer (OEM) IAW CDRL A017 switch manufacturer's required actions for each survey 30 days in advance.

h. The Contractor shall collaborate with the Government to ensure that NEC-provided escorts are available during the complete survey time frame.

7.2 SURVEY AND ENGINEERING

The objective of this task is to provide core survey, engineering, and implementation support for the integration of the ICAN infrastructure IAW the latest version of the DISN ICAN-DI network architecture. Under this contract, the Contractor shall provide the appropriate skill set to gather physical, logical and configuration data of the existing network. The Contractor shall design the Logical ICAN solutions for each US Army B/P/C/S while leveraging DoD US Army and industry standards, technology and service components to the maximum extent possible.

7.2.1 SITE SURVEY SUPPORT

The Contractor shall work directly with the PdM I3MP planning team to complete initial site surveys, perform site survey support activities, and begin detailed, site-specific engineering for the designated B/P/C/S. These activities shall include, but not limited to:

Conduct surveys and gather data (via manual or automated mechanisms/tools) affecting B/P/C/S.

a. The Contractor shall lead the physical site survey of core (ACS/Collection Area Switches/ADS/EAS) locations and document pertinent information necessary to engineer and implement a parallel core; or utilize other methods/architecture. An electrical survey team from TYAD will accompany the Contractor during the core survey to document and engineer power upgrades necessary to install a parallel core.

b. US Army Information Systems Engineering Command (USAISEC) may conduct physical site surveys of End User Buildings (EUBs) with port densities greater than 48 ports for select Telecommunications Rooms (TRs) or verify historical data with NEC from previous site surveys and NETMOD implementations. The Contractor shall utilize the results of the TR surveys to determine IBOM requirements for EAS deployment. The Contractor shall coordinate with I3MP and USAISEC to adjust survey requirements based on known site conditions.

c. Produce Site Survey Report (site-specific equipment and infrastructure requirements, deficiencies and recommendations for rack space, power, HVAC, fiber, etc.) for each B/P/C/S visited.

d. The average survey duration is estimated at two weeks; however, survey duration will be adjusted based on size of the B/P/C/S, information gathered during pre-survey activities and historical data from previous PdM I3MP modernization efforts. The site survey activities for each site are considered complete at the submission of Site Survey Report (SSR) IAW CDRL A001, which will be used as a basis for site preparations and necessary infrastructure upgrades in preparation for installations.

7.2.1.1 ELECTRONIC SITE SURVEY

The Contractor shall perform a 100% electronic logical scan on the network to validate information collected during physical site surveys and historical data is accurate and all active network components are properly identified. The electronic analysis scan will be initiated within two weeks of the start of site engineering efforts at each B/P/C/S. Electronic discovery licensing will be made available to the local NEC/Directorate of Information Management (DOIM) as Contractor remote network access is being processed. The results or data from the Electronic Scan shall be provided with the SSR information and be leveraged to assist in developing the Engineering Installation Plan (EIP) IAW CDRL A015 Electronic discovery licensing will be supported by a software vendor’s application that is certified to be used on the Army’s unclassified network and approved with a valid US Army Certificate of Networthiness (CoN), Risk Management Framework (RMF) Assess Only Process and/or Approved Product List (APL). The Contractor is responsible for providing the required licenses for supporting sites listed

DoD CONUS locations (Attachment 1).

The Contractor shall conduct an electronic scan of the existing network architecture for the Installation Campus Area Network (ICAN) of each B/P/C/S as approved by the USG. The Contractor shall ensure the electronic scan includes, but not limited to the following devices/services:

a. Layer 2 and Layer 3 network elements, Anonymous Devices, Non-NEC managed devices connected to the NEC, Tenant Managed or “Shadow DOIM” Devices.

b. Layer 2 extensions between core switches and NEC Firewall, core switches and TLA Firewall, and core/distribution switches to Tenant.

c. End user devices, Server Farms, 802.1x, VTC, SCADA, Multicast, and applications as applicable.

d. Capability to discover network devices, configuration data and record the processed data.

e. System Documentation to include an inventory and documentation of network configuration, servers, software, network connectivity and other components.

f. Comprehensive Assessment that includes analysis of the full spectrum of network characteristics.

g. The Contractor shall ensure that assigned network engineers are properly authorized, trained and certified for full privilege (read-write) access to ICAN network devices and management tools to provide on-site and/or remote analysis of the network.

h. The Contractor shall ensure proper handling of the ICAN configuration data collected with the enterprise analysis tool.

i. Applications processing the data on an Army owned system must be approved by the Government and operate within the limits of the Approval Authority (AO).

j. The database will not exceed aggregated information from more than two B/P/C/S at one time. Once the fielding from a designated B/P/C/S installation is complete, the information will be removed from the database immediately and deposited via DVD in an approved GSA safe.

k. Applications processing the data on a Vendor owned system must reside in an offline lab environment that is not connected or accessible from the Internet

without specific written approval from USG.

l. All personnel having access to this information on Non-Classified (Non-Secure) Internet Protocol Router Network (NIPRNET) will have the appropriate security clearance (minimum SECRET) in place and must sign appropriate non-disclosure agreements (NDA) before access is granted.

m. Contracted integrators may only retain copies of the data for the duration and scope of their contract.

n. At any time, the USG may inspect the facilities being used to store and process the data. Remote analysis is only authorized at approved B/P/C/S designated by USG. The Contractor shall ensure remote access to NIPRNET resources is approved and complies with NSA, DoD policies, guidelines and DISA STIGs.

7.2.2 ICAN ENGINEERING SUPPORT

The Contractor shall provide ICAN engineering support activities to include, but are not limited to, the following:

a. Develop an installation-specific Engineering Installation Package (EIP) IAW CDRL A015 and solution for implementation for the ICAN switches. The Contractor's Engineering Team shall provide the fielding engineers all of the necessary information required to perform the implementation action.

b. Each EIP shall include at a minimum:

- "As-Is" and "To-Be" Physical and Logical Network Architecture
- Integration Plan
- Information Assurance (IA) artifacts: Security Technical Implementation Guide (STIG) Checklist, Internetwork Operating Systems (IOS) versions, Plan of Action & Milestones (POA&M), list of Hardware and Software, etc.
- Test Plan(s)
- Data Connectivity Plan
- Implementation Plan
- Transition/Migration Plan
- Installation Team Checklists

- Utilize US Army Engineering processes during the development of all submissions; identify additional processes and documentation formats, as necessary.

c. Submit site-specific EIP to USG for review and approval. Adhere to USG established process for reviewing, updating, approving and disseminating EIP throughout its lifecycle and versioning from inception (EIP version 1.0) to final pre implementation (EIP version 3.0) and the final “As-Built Implementation” that is completed post implementation to document any changes that occurred during implementation.

d. Conduct early operational assessments, developmental testing, operational testing, and evaluation of IT systems. Standard ICAN testing will include (1) Network Connectivity; (2) STIG and Information Assurance Vulnerability Alert (IAVA) compliance; (3) Domain Access; (4) Global Internet Connectivity; (5) Enterprise Email and (6) Access to all other Services.

e. Provide remote support to assist during the ACS/ADS/EAS migrations.

7.3 PRE-IMPLEMENTATION ACTIVITIES

The Contractor shall collaborate with the Government to complete the following items before the implementation activities take place:

a. Automated network survey results will be greater than 90 percent complete prior to the implementation date.

b. The NEC will supply hostname information prior to EIP Version 2.

c. All facility work (power, HVAC, shelter and OSP fiber) that is required for the network's effort will be complete by the scheduled EIP submission date.

d. The Contractor shall collaborate with the Government to identify the BDE resources and trail boss no later than three weeks prior to implementation.

e. All passive and consumable materials will be onsite a minimum of 20 days before the implementation, and will have been inventoried.

f. Travel Authorization Requests will be approved at least ten days prior to implementation travel date.

g. The NEC and the BDE will produce the initial ASI schedule at least two weeks before the EAS deployment.

h. JB-CE routers will be installed and commissioned prior to the implementation effort.

i. The B/P/C/S NMS will be stable and static upon commencement of the installation. All 802.1X, AAA, ACS, etc. systems will be installed and 100 percent operational prior to installation of the Networks hardware.

j. The Contractor shall collaborate with the Government for the purpose of granting B/P/C/S network access during the entire implementation effort.

k. The Contractor shall collaborate with the Government for the purpose of ensuring that no on-going B/P/C/S project is underway to interfere with the Contractor's implementation of the ACS devices.

l. The Contractor shall collaborate with the Government for the purpose of ensuring that ACS and ADS implementations can be performed in parallel without an Authorized Service Interruption (ASI).

m. The Contractor shall collaborate with the Government for the purpose of ensuring that NEC-provided escorts are available during the complete implementation timeframe.

7.4 ICAN INSTALLATION AND CONFIGURATION TESTING

The objective of this effort is to deliver an ICAN infrastructure capable of serving the needs of a specific B/P/C/S. This infrastructure shall be designed and deployed IAW the established and latest version of US Army DISN ICAN-DI architecture. The Contractor shall develop and apply systems engineering methodology towards the installation, configuration and testing of the ICAN network infrastructure upgrade.

Implementation efforts are considered complete when the Contractor has: (1) installed and made operational the ACS core, (2) successfully migrated existing route points to the JB-CE routers, (3) completed the 30-day window for remote support, which commences upon the Contractor's departure from each B/P/C/S, and (4) submitted EIP version 4.0, including as-built configurations, to PdM I3MP TMD and ISEC. NEC and BDE resources are responsible for completing the continued ADS/EAS deployments on each B/P/C/S.

The Contractor shall install network hardware identified in the EIP. The Contractor shall participate in the identification of the core ACS hardware required for the NEC-controlled server farm and shall provide guidance to the Government in terms of installation and base configuration in support of the ACS.

7.4.1 ACS INSTALLATION AND CONFIGURATION TESTING

The Contractor shall perform ACS switch installations, configuration and testing, ramping up to support four (4) simultaneous ACS/ADS/EAS installation teams. These activities will include, but not be limited to, the following:

a. Coordinate with PdM I3MP to confirm detailed design from the survey and engineering team and equipment availability.

b. Coordinate with the local NEC and RCC-C for Authorized Service Interruption (ASI) window availability.

c. Support Tobyhanna Army Depot (TYAD) with calculating the additional power materials required for ACS installation based on data identified during survey.

d. Coordinate all resources necessary to successfully complete the installation requirements.

e. Install GFE Uninterruptible Power Systems (UPS) as identified in EIP. Coordinate with electrical contractors for installation of hard-wired UPS systems.

f. Install ACS switches, modules and interfaces to support US Army ACS/ADS/EAS architecture (may include physical lifting and installation of equipment).

g. Perform in network “Roll Back” in case of migration difficulties.

h. Apply switch configurations.

i. Verify connectivity to Network Management System (NMS).

j. Conduct testing and evaluation of ACS latest IOS versions, as required. This includes configuration testing and patching necessary to provide compliance to the latest STIGs and IAVAs.

k. With B/P/C/S NEC and BDE resources, support ACS pre-patching as required for all ACS/ADS facilities including the fiber/cable labeling schema identified in the Hostname builder spreadsheet in the EIP.

l. Provide on-site management support during initial implementation activities to ensure the engineering team has appropriate resources and representation during NEC/BDE prep/coordination meetings.

m. Coordinate on-site installation with direct current (DC) electrical contractor as required to ensure DC powered ACS equipment can be installed at each

B/P/C/S. The IMS shall be updated by the Contractor to ensure both resources are available to complete DC power work on-site at the same time.

n. Provide reconfiguration support (rework) as required to correct non-standard configurations produced by NEC installation plans executed prior to EIP hand- off and NEC installation plans that differ from what is recommended in the EIP.

o. Provide base JB-CE MPLS Router configurations and base code (iOS) upgrade support as required.

p. Provide support as required to obtain IA approval for DISA router including STIG configuration files.

q. Provide coordination with RCC-C as required to obtain access credentials for remote network access to manage legacy and new DISA and Network ACS/ADS/EAS devices.

r. Conduct standard post-installation Quality Assurance (QA) testing that will include (1) Network Connectivity; (2) Domain Access; (3) Global Internet Connectivity; and access to other services such as (4) Enterprise Email.

s. Provide post-install support, including finalizing as-built documentation and provide training and transition support.

t. Provide As-Built documentation to support Asset Management Configuration Management (CM) updates to reflect the post-installation status.

7.4.2 EAS INSTALLATION AND CONFIGURATION TESTING

The Contractor shall provide SME assistance to the EAS NEC106th SB, 93rd SB and 21st SB implementation teams in the ADS/EAS installation, configuration and testing. These activities will include, but are not limited to, the following:

a. Coordinate with designated PdM I3MP site representative to confirm detailed design from the EIP, equipment availability and ASI window availability

b. Support ISEC with identifying the passive materials required for ADS/EAS installation based on survey data identified in the ISEC SRS deliverable.

c. Support TYAD with calculating the additional power materials required for EAS installation based on data identified during the survey.

d. Implement switch configurations and provide on-site hands-on-training to the

ADS/EAS BDE Implementation Team for configuring ADS/EAS switches.

e. In coordination with ADS/EAS SB implementation team, assist in initial install of ADS/EAS switches and provide SME technical support to the ADS/EAS SB implementation team for installing remaining EAS switches, modules, and interfaces to support US Army ACS/ADS/EAS architecture (may include physical lifting and installation of equipment). The Contractor SMEs will provide training that will enable the ADS/EAS SB implementation team to complete the configuration and installation of the remaining ADS/EAS switches.

f. Perform full “proof-of-concept testing with local NEC in the beginning phase of EAS deployment to confirm all protocols and services are functioning and final configurations are ready to deploy.

g. In coordination with ADS/EAS SB Implementation team, assist in network “Roll Back” in case of migration difficulties.

h. Verify connectivity to NMS.

i. Coordinate resources, as necessary, to successfully complete installation, configuration, and testing requirements.

j. Execute test plan for: (1) Network Connectivity; (2) STIG and IAVA compliance; (3) Domain Access; (4) Global Internet Connectivity; (5) Enterprise Email; and (6) Access to all other Services.

k. Provide post-install support, including finalizing As-Built documentation IAW CDRL A003, and provide training and transition support, IAW CDRL A012 as required.

l. Provide final electronic scan of the network utilizing the approved discovery application supported during electronic survey to capture all new hardware installed and incorporate into the final version of the EIP to represent the “As-Built”. Final hardware count will be briefed to PdM I3MP/TMD staff.

m. Conduct testing and evaluation of latest ADS/EAS IOS versions, as required. This includes configuration testing and patching necessary to provide compliance to the latest STIGs and IAVAs.

7.4.3 EDGE INSTALLATION SUPPORT

The Contractor shall provide training and support to assist the B/P/C/S NEC, BDE and BMM resources with ADS/EAS installations. These activities will include, but are not

limited to, the following:

a. The Contractor shall coordinate with designated B/P/C/S representatives to confirm equipment availability, Installation Bill of Materials (IBOM) IAW CDRL A016, availability and ASI window availability.

b. The Contractor shall provide switch configurations to the NEC via EIP and shall work with the NEC to complete remaining EIP issues – including HOSTNAME location updates and prep work that needs to be coordinated with NEC Network Resources.

c. The Contractor shall provide recommendations to designated NEC and BDE resources to prepare staging areas processes for configuration and deployment of the remaining EAS switches to support the approved US Army ACS/ADS/EAS architecture. Contractor shall develop a Staging Plan.

d. The Contractor shall assist designated NEC and BDE resources with installing the remaining EAS switches, modules and interfaces to support the US Army ACS/ADS/EAS architecture.

e. The Contractor shall verify ACS/ADS/EAS connectivity to NEC NMS resources.

f. The Contractor shall coordinate resources as necessary, to successfully complete the installation, configuration and testing requirements.

g. The Contractor shall conduct standard post-installation QA testing that will include (1) Network Connectivity; (2) Domain Access; (3) Global Internet Connectivity and access to other services such as (4) Enterprise Email.

h. The Contractor shall provide post-install support, including finalizing As-Built documentation IAW CDRL A003, providing training and transition support, as required.

7.4.4 EDGE ACCESS SWITCH INSTALLATION

The current plan is for NECs, Signal Brigades and BMM if available to install EAS after the parallel core or other proposed method/architecture has been installed by the Contractor. The Contractor shall have the capability to install EAS (Attachment 2) in lieu of BMM on an as needed basis, with Government direction.

7.5 NON-CLASSIFIED INTERNET PROTOCOL (IP) ROUTER NETWORK (NIPRNET)

The Contractor shall support the survey, engineering and implementation of the B/P/C/S NIPRNET ICAN, including Area Core Switches (ACS), Collection Area Switches, Area Distribution Switches (ADS) and Edge Access Switches (EAS) as defined in the latest version of the DISN ICAN-DI architecture document. The Contractor shall survey, engineer, install, configure, test and make operational a parallel core (ACS/Collection Area Switches/ADS); or propose other methods and architecture at assigned B/P/C/S that will facilitate and ease the migration of new EAS by NEC, Brigade and Borrowed Military Manpower (BMM). The new parallel ICAN core or other method/architecture requires interfaces to Joint Base Customer Edge (JB-CE) or other collection routers based on site conditions.

The JB-CEs on a B/P/C/S could require:

a. Full replacement – the Contractor shall survey, engineer, install, configure, test and make operational parallel JB-CE routers provided as Government Furnished Equipment (GFE) based on the Joint Multiprotocol Label Switching - Outer Core (JMPLS-OC) Standards and Specifications.

b. Upgrade the existing B/P/C/S JB-CEs, if necessary, with GFE line cards for supporting a new parallel core infrastructure.

c. Utilize existing JB-CE routers capable of supporting a new parallel core infrastructure.

The Contractor shall coordinate with the NEC, Regional Cyber Center-CONUS (RCC-C) and DISA to establish necessary interfaces on either new or existing JB-CEs to enable the parallel ICAN core or other proposed method/architecture.

7.6 SECRET IP ROUTER NETWORK (SIPRNET) ICAN MODERNIZATION

The Contractor shall have the capability to support optional tasks to survey, engineering and implementation of the B/P/C/S SIPRNET ICAN modernization in accordance to the latest version of the DISN SIPRNET-ICAN-DI architecture document. The Contractor shall support requirements that are similar to those for NIPRNET ICAN as specified in Sections 7.1 through 7.5, but to a lesser extent due to the smaller footprint of SIPRNET ICANs.

7.7 NEXT-GENERATION NIPRNET ICAN MODERNIZATION

The Contractor shall have the capability to support optional tasks to survey, engineering and implementation of the Next-Generation NIPRNET ICAN modernization in accordance to the to-be-released version 2.0 of the DISN NIPRNET-ICAN-DI architecture document, which will utilize software-defined network (SDN) architecture and technologies.

8.0 CERTIFICATION & ACCREDITATION (C&A) SUPPORT

The Contractor shall provide IA support activities. These activities shall include, but are not limited to, the following:

a. Assist in the development of a standard baseline configuration for each device using the latest DISA STIGs and applicable IAVA patches.

b. Support the ACS/ADS/EAS IOS upgrades with regard to Security and IT C&A services.

c. Support the US Army in creating the Cyber Security package using the RMF process.

9.0 SITE RESCHEDULING

Customer requirements for I3MP Government control and accountability may dictate changes to the sites and/or schedule as required. If determined by the Government that the proposed sites will change, the Government shall collaborate with the Contractor as soon as possible. The Government shall collaborate with the Contractor for the purpose of ensuring and providing a reasonable amount of time and information to readdress the presented proposal and pricing structure to address factors of analysis, geographical distance, existing equipment and systems, work to be performed, technical solution, travel cancellations, site complexities and ongoing project de-conflicting activities.

10.0 GOVERNMENT FURNISHED SERVICES MATERIALS

The Contractor shall collaborate with the Government for the purpose of gaining access to USA facilities, including physical access, network access, system access and required credentials (i.e., CAC [Common Access Card], administrative accounts) to allow the Contractor’s technical staff to complete the assigned GFE network device replacements. In addition, the Contractor shall collaborate with the Government for the purpose of identifying B/P/C/S designated representatives that shall provide access or arrange for an escort to enable the Contractor’s technical staff to access the switches to

be replaced. The Contractor shall collaborate with the Government for the purpose of ensuring that the required Logistics support assets at the Government furnished warehouse are received and accounted for and then the re-shipped ACS/ADS/EASs back to designated locations.

Contractors shall be provided GFE laptops necessary to complete the efforts on this contract. The GFE equipment shall utilize an Army Gold Master (AGM) image connected to and managed by the Ft Belvoir NEC under the North American East (NAE) domain. The Contractor shall not have administrative privileges to the laptops and shall maintain cyber security patches/domain log-in rights IAW NEC and ARCYBER policies via either direct connection or remote access via Virtual Private Network (VPN) software. The Contractor shall maintain IA training requirements and sign appropriate Acceptable Use Policy (AUP) agreements as required.

The Contractor shall submit DD Form 2875, System Access Request (SAR) for employees requiring an NAE account necessary to conduct daily official business with the Government in the performance of this contract for approval. Additional DD 2875 forms may be required for elevated privilege accounts and shall be approved on an as-required basis.

11.0 OTHER DIRECT COSTS/TRAVEL

Under this effort, allowable Other Direct Cost (ODC) will be included, such as travel costs, to support installation efforts, as required by the Government. Written Government approval must be obtained by the Contractor prior to ODC purchases and/or incurred costs, including the explicit approval for cost of materials, shipping, etc. The Contractor shall submit a minimum of three cost estimates for ODC materials that are at or below the minimum micro-purchase threshold as specified in FAR Part 2.101 and may not exceed the micro-purchase threshold unless authorized by the Government.

The cost of general purpose items required for the conduct of the contractor's normal business operations will not be considered an allowable ODC in the performance of this contract. All ODCs must have Government approval/authorization by the Contracting Officer or designated COR prior to expending funds. The ODC CLIN will be cost reimbursable and non-fee bearing. No profit, fringe, material handling, pass-through costs, or any other markup is allowed.

Travel for the ACS/ADS/EAS team to support the Survey and Engineering Team and ACS/ADS/EAS Implementation Teams for each B/P/C/S are identified in DoD CONUS locations (Attachment 1).

Attachment 1 provides the survey, engineering and implementation locations. For planning purposes, the Contractor shall plan two weeks for each survey (i.e., travel on Monday; survey Tuesday, Wednesday, and Thursday; travel on the following Friday dependent on the size of the B/P/C/S). The DoD CONUS locations (Attachment 1) provides the planned locations identified within the IMS. Estimated number of ACSs and EASs for each designated B/P/C/S are also displayed on DoD CONUS locations (Attachment 1). The implementations will be completed during a five-day work week. Air travel will not be used for travel to Aberdeen Proving Grounds (APG) MD, Ft Meade MD, Ft Detrick, MD and/or Ft Belvoir, VA.

Travel arrangements shall be IAW the PWS requirements. Travel arrangements for Contractor personnel shall be provided to and approved by the COR or KO in advance of travel. All extended travel must be approved by the COR/KO prior to the commencement of travel. All travel must be IAW applicable command policies as well as the Joint Travel Regulation (JTR), US Army Form Pamphlet (PAM) 715-16, Army Regulation (AR) 715-9 and the limitation of funds executed on this contract. Reimbursement for the cost of lodging and incidental expenses will be actual costs incurred and shall be considered reasonable and allowable provided that the actual cost does not exceed the rates and amounts allowed IAW the law and JTR, local command policy PAM 715-16 and AR 715-9, when applicable. Using Government funds to pay for premium-class travel (first and business) is strictly prohibited.

The Government intends to provide all of the necessary materials, supplies and equipment necessary for the Contractor to complete the implementation of the B/P/C/S identified in this effort. However, it is anticipated that the contractor may be required to obtain limited materials or incur limited expenses in performance under the contract. The Contractor shall propose a reasonable estimate for these items as an ODC on an as needed basis. All items will require approval from the COR prior to purchase. The Contractor shall not be reimbursed for any items that were not specifically authorized or approved by the COR.

12.0 SECURITY REQUIREMENTS

The nature of this PWS requires access to US Army unclassified systems. The Contractor’s assigned responsibilities mandate access to classified spaces. All Contractor personnel who will perform work onsite are required to be eligible to obtain and maintain a minimum of Secret clearance on file. Network engineering and command center support staff who will require administrative access (read-write) to the B/P/C/S networks must meet the criteria of 8570.1 and have an active Top Secret (TS) clearance, as directed by the Army. Vendor and IA certifications must be registered in the Army’s ACTCS account tracking system. Contractor personnel must be U.S. citizens

and possess at least an interim security clearance to begin work on this effort. Additional security requirements will be stipulated in the DD Form 254 for the basic contract to be provided by the Government at contract award.

The Contractor and all associated Subcontractor employees shall comply with applicable installation, facility, and area commander installation and facility access and local security policies and procedures USG. The Contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by the installation Provost Marshal Office, Director of Emergency Services, or Security Office. The Contractor's workforce must comply with all personal identity verification requirements as directed by DoD, Headquarters Department of the Army (HQDA) and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the USG may require changes in Contractor security matters or processes.

12.1 SPECIAL SECURITY REQUIREMENTS

The following paragraphs identify the security requirements, where applicable, for this effort. All training performed in association to the security requirements below shall be reported in an Operations Security (OPSEC) Report IAW CDRL A009 of this PWS. The OPSEC Report shall include the status of all security training required, taken and planned, IAW the time frames specified within the PWS. The report shall include each Contractor and Subcontractor employee assigned to each site.

12.1.1 ANTI-TERRORISM (AT) LEVEL I AWARENESS TRAINING

All Contractor and Subcontractor employees requiring access to Army installations, facilities or controlled access areas shall complete AT Level I awareness training within 30 (or less) business days after contract start date or date of hire on the contract. The Contractor shall submit a certificate of completion for all personnel affected to the USG within ten business days after completion of training. AT Level I, awareness training is available at the following website: http://jko.jten.mil.

12.1.2 ACCESS AND GENERAL PROTECTION/SECURITY POLICY AND PROCEDURES

The Contractor and all associated Subcontractor employees shall provide all information required for background checks to meet installation access requirements to be accomplished by the installation Provost Marshal Office, Director of Emergency Services or Security Office. The Contractor workforce must comply with all personal identity verification requirements (IAW the FAR) as directed by DoD, Headquarters

Department of Army (HQDA) and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the FPCON at any individual facility or installation change, the Government may require changes in Contractor security matters or processes.

The Contractor and all associated Subcontractor employees shall comply with applicable installation, facility and area commander installation and facility access and local security policies and procedures.

The Contractor and USG will discuss all security issues in a pre-facilities meeting on-site prior to any commencement of facilities related work.

12.1.3 CONTRACTORS/SUBCONTRACTORS REQUIRING COMMON ACCESS CARD (CAC)

U.S. Army Installations participate in a standardized entry protocol. The Contractor shall enroll all employees that require routine access. The Contractor shall be responsible for providing all necessary and accurate information to obtain and maintain enrollment in the base/facility access system. The Contractor shall also be responsible for ensuring that the personnel enrolled remain enrolled during the entire period of performance in which that Contractor/employee is needed. The Contractor shall meet all requirements identified by the Office of the Garrison Commander in compliance with any installation policy memorandum. In the event that there are changes to any Contractors and/or employees thereof, the Contractor shall notify the USG and ensure enrollment is properly updated.

Before CAC issuance, the Contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05. The Contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of six months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the Federal Bureau of Investigations (FBI) fingerprint check and a successfully scheduled NACI at the Office of Personnel Management (OPM).

12.1.4 CONTRACTORS/SUBCONTRACTORS NOT REQUIRING CAC, BUT REQUIRE ACCESS TO A DOD FACILITY OR INSTALLATION

The Contractor and all associated Subcontractor employees shall comply with

adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by Government representative).

12.1.5 AT AWARENESS TRAINING FOR CONTRACTOR PERSONNEL TRAVELING OVERSEAS

US based Contractor employees and associated Subcontractor employees shall make available and receive Government provided Area of Responsibility (AOR) specific AT awareness training as directed by AR 525-13. Specific AOR training content is directed by the Combatant Commander with the unit Authority to Operate (ATO) being the local point of contact.

12.1.6 IWATCH TRAINING

The Contractor and all associated Subcontractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO), as applicable to the site. This training is used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the USG. This training shall be completed within ten (10) business days of contract award and within five (5) calendar days of new employees' commencing performance, the results shall be reported to the USG no later than five (5) calendar days after contract award.

12.1.7 ARMY TRAINING CERTIFICATION TRACKING SYSTEM (ATCTS)

All Contractor employees with access to a Government information system must be registered in the Army Training Certification Tracking System (ATCTS) at commencement of work, and must successfully complete DoD Information Assurance Awareness prior to access to the information system and then annually thereafter.

12.1.8 OPERATIONS SECURITY SOURCE STANDARD OPERATING PROCEDURE PLAN

The Contractor will develop an Operations Security Source (OPSEC) Standard Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC Officer, per AR 530-1, Operations Security IAW the CDRL A009 of this PWS. This plan shall include a process to identify critical information, where it is located, who is responsible for it, how to

protect it and why it needs to be protected. The Contractor shall implement OPSEC measures as ordered by the Commander. In addition, the Contractor shall have an identified certified Level II OPSEC coordinator per AR 530-1. The Contractor shall submit an OPSEC SOP/Plan, IAW CDRL A009 to address the manner in which all training required by contract and/or local safety and security guidelines and policies is delivered, documented and maintained.

12.1.9 OPSEC TRAINING

Per AR 530-1, Operations Security, all Contractor employees must complete Level I OPSEC Awareness Training. New employees must be trained within 30 business days of reporting for duty and annually thereafter. Level I OPSEC Awareness Training is available at Security Awareness Hub (usalearning.gov). https://securityawareness.usalearning.gov

12.1.10 INFORMATION ASSURANCE (IA)/IT TRAINING

All Contractor employees and associated Subcontractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All Contractor employees working IA/IT functions must comply with DoD and Army training requirements IAW DoD 8570.01, DoD 8570.01-M and AR 25-2, at the time of appointment to IA/IT functions.

12.1.11 IA/IT CERTIFICATION

Per DoD 8570.01-M, DFARS and AR 25-2, the Contractor employees supporting IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award.

12.2.12 AUTHORIZED TO ACCOMPANY THE FORCE

Not Applicable.

12.2.13 PERFORMANCE OR DELIVERY IN A FOREIGN COUNTRY

Not Applicable.

12.2.14 HANDLING OR ACCESS TO CLASSIFIED INFORMATION

The Contractor shall comply with the FAR for security requirements. This involves access to information classified “Confidential”, “Secret” or “Top Secret” and requires all Contractors and its employees to comply with the Security Agreement (DD Form 441),

including the National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M and any revisions to DoD 5220.22-M, notice of which has been furnished to the Contractor.

12.2.15 THREAT AWARENESS REPORTING PROGRAM (TARP) TRAINING

For all Contractors with a security clearance per AR 381-12 Threat Awareness Reporting Program (TARP). Contractor employees must receive Annual TARP training by a Counter Intelligence (CI) agent or other trainer. The Contractor will provide a certified list of all contract personnel and dates of completion. Training will be schedule within 30 days of contract award or 30 days of a new employee commencement date.

12.2.16 SAFEGUARDING USG EQUIPMENT, INFORMATION AND PROPERTY

The Contractor shall be responsible for safeguarding all USG equipment, information and property provided for Contractor use. If the Contractor receives access and responsibility for the security of a USG facility, at the close of each work period, the Contractor shall secure those facilities, equipment and materials.

12.2.17 CYBERSECURITY (CS)

The use of commercial Internet Service Providers (ISPs) or e-mail accounts (e.g. Hotmail, Yahoo, Gmail, etc.) for official purposes is prohibited. Contractors shall implement encryption and/or control communication measures for official business appropriate for the sensitivity of the information transmitted. There is no prohibition for manually forwarding email messages, ONE AT A TIME, after opening and reading the content to ensure that the information is not sensitive or classified.

The Contractor shall comply with the DoD Risk Management Framework (RMF) and verify that the enclave, system or network is prepared to undergo Authorization. The Contractor shall verify that the addition of any hardware or software to the enterprise network are configured in such a manner as to ensure enterprise process and standards comply with current DoD CS policy and more specifically RMF requirements.

All RMF requirements shall be met for that portion of the system NLT ten business days prior to preliminary System Acceptance (SAT) and connection to the LAN of any portion of the overall system. The contractor shall provide the configuration file from applicable devices to the I3MP Information System Security Manager (ISSM) showing implementation of the Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG) and/or Military Unique Deployment Guide (MUDG) prior

to connection to the LAN of any portion of the overall system.

The Contractor shall be responsible for systems patching and hardening according to DISA, Army/DoD MUDG and local command/system owner guidelines. Contractors shall have SME personnel available to provide root level access to systems for final validation and make changes for any findings as necessary. Contractors are required to develop a Plan of Action and Milestones (POA&M) IAW RMF requirements for systems requiring corrective actions/remediate and/or mitigation/resolution alternatives with associated risk. The Contractor shall implement a monitoring and patching process at a minimum 30 day interval ensuring validated systems remain compliant after initial validation Systems requiring a version change of software/firmware as a resolution for findings require configuration control review prior to the change.

If applicable, the Contractor shall comply with the Army Computer Hardware, Enterprise Software and Solutions (CHESS) requirements to the fullest extent possible. Otherwise, when buying electronic parts the Contractors shall, whenever possible, buy electronic parts from the Original Component Manufacturer (OCM) or their authorized distributor(s). If applicable, the Contractors shall provide supply chain traceability documents to OCM for all Item Unique Identification (IUID) items, ten calendar days after award. The Contractors shall provide a completed DISA STIG checklist that is applicable to the proposed systems or products prior to acquiring the equipment.

The Contractor shall be responsible for safeguarding all USG equipment, information and property provided for Contractor use. If the Contractor receives access and responsibility for the security of a USG facility, at the close of each work period, the Contractor shall secure those facilities, equipment and materials. The Contractor and the USG shall discuss all safety, security and force protection issues in a pre-facilities meeting onsite prior to any commencement of facilities-related work.

12.1.18 ANTI-TERRORISM COMPLIANCE

The Contractor shall adhere to the applicable DFARS clauses. This applies to both contingency and non-contingency support. The key AT requirement is for non-local national Contractor personnel to comply with theater clearance requirements and allows the Combatant Commander to exercise oversight to ensure the Contractor’s compliance with Combatant Commander and Subordinate Task Force Commander policies and directives.

12.1.19 COMBATING TRAFFICKING OF PERSONNEL TRAINING

The Contractor, Contractor employees, and all Subcontractors shall comply with the applicable FAR clauses. The Contractor shall maintain a Certification Regarding

Trafficking in Persons Compliance Plan during the performance of the contract. The compliance plan must include, at a minimum, the following:

An awareness program to inform Contractor employees about the Government's policy prohibiting trafficking-related activities described in paragraph (b) of this clause, the activities prohibited, and the actions that will be taken against the employee for violations. Additional information about Trafficking in Persons and examples of awareness programs can be found at the Web site for the Department of State's Office to Monitor and Combat Trafficking in Persons at http://www.state.gov/j/tip/.

A process for employees to report, without fear of retaliation, activity inconsistent with the policy prohibiting trafficking in persons, including a means to make available to all employees the hotline phone number of the Global Human Trafficking Hotline at 1-844-888-FREE and its email address at help@befree.org.

A recruitment and wage plan that only permits the use of recruitment companies with trained employees, prohibits charging recruitment fees to the employee, and ensures that wages meet applicable host-country legal requirements or explains any variance.

A housing plan, if the Contractor or Subcontractor intends to provide or arrange housing that ensures the housing meets host-country housing and safety standards.

Procedures to prevent agents and Subcontractors at any tier and at any dollar value from engaging in trafficking in persons (including activities in paragraph (b) of this clause) and to monitor, detect, and terminate any agents, subcontracts, or Subcontractor employees that have engaged in such activities.

The Contractor shall submit certificates of completion for Combating Trafficking in Persons (CTIP) Training for each Contractor employee and Subcontractor employee to the USG within ten business days after completion of training.

13.0 ACCIDENT/SAFETY REPORTING INVESTIGATIONS

Occupational deaths, injuries and illnesses sustained by the Contractor while conducting work on this delivery order, will be reported, investigated and analyzed in accordance with AR 385-10 and DA PAM 385-40. Investigations will focus on the root causes, contributing factors, lessons learned and actions taken to prevent recurrence. The Contractor shall report all Incidents that meet the Commander’s Critical Information Requirement (CCIR) criteria and shall be reported promptly, and may require a proper accident investigation.

The Contractor shall report Injuries resulting in day(s) away from work, restricted duty

and/or medical treatment beyond first aid will be documented on the DA Form 285-AB, US Army Abbreviated Ground Accident Report (AGAR) and submitted via "ReportIt", the single US Army accident and risk management system – https://reportit.safety.army.mil/ **within 48 hours of injury occurring.** The Contractor shall submit AGARs and the action will be routed directly to the COR for review and concurrence. Final review and concurrence will be conducted by the US Army Safety Director.

The Contractor will ensure internal accident reporting processes are in place at all times Processes should include notification to the COR, organization safety officers, and the local Garrison/Installation Safety Office. Work directly with your assigned Safety Officers to implement and comply with these requirements. Employees will report all workplace incidents, regardless of the severity to their immediate supervisor and COR.

14.0 ACS/ADS/EAS ENGINEERING DELIVERABLES

The Contract Deliverable Requirements List (CDRLs) required by this Task Order are identified in Table 1.

CDRL	PWS Para #	Description	DID Number	DID Title
A001	7.2.1	Site Survey Report (SSR)	DI-MISC-81381	Site Survey Report
A002	7.1.1	Government Property Inventory Report	DI-MGMT-80441C	Procurement List of Materials (LOM)
A003	7.2.2, 7.4.2, 7.4.3	Real Property As-Built Drawings	DI-MISC-81489A	As-Built Drawings
A004	7.1.1	Briefing Materials	DI-MGMT-81605	Briefing Materials
A005	7.1.1	Integrated Program Management Report (IPMR)	DI-MGMT-81861A	Integrated Master Schedule (IMS)
A006	7.1.1	Management Plan	DI-MGMT-80004A	Project Management Plan (PMP)
A007	7.1.1	Quality Assurance Program Plan	DI-QCIC-81794A	Quality Management Plan (QMP)
A008	7.1.1	Contractor's Risk Management Plan	DI-MGMT-81808	Risk Management Plan
A009	7.1.1	Operations Security (OPSEC) Plan	DI-MGMT-80934C	OPSEC SOP/PLAN

A010	7.1.1	Contractor's Safety Plan	DI-SAFT-82080/T	Accident Prevention/Safety Plan
A011	7.1.1	Configuration Management Plan (CMP)	DI-SESS-81875	Configuration Management Plan (CMP)
A012	7.1.1	Syllabus	DI-MISC-81459A/T	Training Plan
A013	7.1.1	Acceptance Test Report	DI-QCIC-81891	Technical Acceptance Report
A014	7.1.1	Government Property Inventory Report	DI-MGMT-80441C	Major Bill of Materials (MBOM)
A015	7.2.1.1	Site Preparation Requirements and Installation Plan	DI-MGMT-8033A	Engineering Installation Plan (EIP)
A016	7.4.3	Government Property Inventory Report	DI-MGMT-80441C	Installation Bill of Materials (IBOM)
A017	7.1.3	Contractor Furnished Material (CFM) Report	DI-MGMT-82049	Final LOM Physical Inventory
A018	7.1.1	Status Report	DI-MGMT-80368A/T	Weekly Status Report

Table 1: Contractor Data Requirements List (CDRL)

16.0 GENERAL INFORMATION

16.1 INSPECTION AND ACCEPTANCE

Inspection and acceptance criteria for all deliverables shall adhere to the methods standards outlined in the attached Quality Assurance Surveillance Plan (QASP). The Contractor shall submit quarterly reports addressing its performance against the plan and shall address the Contractor's Quality, Completeness, Timeliness, Accuracy, Efficiency, and Effectiveness.

16.2 RECOGNIZED FEDERAL HOLIDAYS

The Contractor is not required to perform services on holidays.

New Year's Day	Labor Day
Martin Luther King's Birthday	Columbus Day
President's Day	Veteran's Day

Memorial Day Juneteenth Thanksgiving Day

Independence Day Christmas Day

16.3 HOURS OF OPERATION

In general, the contractor is responsible for conducting business between the hours of 0800 and 1700, Monday thru Friday – with the exception of the above listed Federal holidays or in the event of a Government facility closure due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor may need to work alternative hours in conjunction with the operational tempo of the tasking and needs of the work/area assigned. The contractor will not be reimbursed for work performed when the Government facility is officially closed. For other than firm fixed price contracts, the Contractor will not be reimbursed when the Government facility is closed for the above reasons. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

Performance of Services during a crisis declared by the President of the United States, the Secretary of Defense, or Overseas Combatant Commander: The performance of these services is not considered to be mission essential during a time of crisis with exception to those performed in declared combat zones. Should a crisis be declared, the Contracting Officer or his/her representative will verbally advise the contractor of the revised requirements, followed by written direction.

16.4 QUALITY MANAGEMENT PLAN

The Contractor shall develop and maintain an effective quality control program to ensure services are performed IAW this PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's quality control program is the means by which he assures himself that his work complies with the requirement of the contract. After acceptance of the quality control plan the contractor shall receive the Contracting Officer's acceptance in writing of any proposed change to his QC system.

16.5 QUALITY ASSURANCE

The Government shall evaluate the Contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the contractor has performed in

accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

16.7 CONTRACT OFFICER REPRESENTATIVE (COR)

The COR will be identified by separate letter. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the Contractor concerning technical aspects of the contract; issue written interpretations of technical requirements, including Government drawings, designs, specifications; monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of Government furnished property, and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

16.8 IDENTIFICATION OF CONTRACTOR EMPLOYEES

All Contract personnel attending meetings, answering Government telephones, and working in other situations where its contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. All documents or reports produced by Contractors must be suitably marked as Contractor products or that Contractor participation is appropriately disclosed. All Contractor personnel will be required to obtain and wear badges in the performance of this service.

16.9 RELIEF AND REMOVAL OF CONTRACTORS

The USG has the authority to relieve and/or permanently remove Contractors for any acts that put at risk the life, safety or health of installation personnel. Contractors permanently “barred from post” will no longer be permitted entry into the installation to include the installation perimeter. All issues of Contractor dismissal or removal shall be reported to the KO within 48 hours of occurrence.

16.10 REPLACEMENT OF RELIEVED PERSONNEL

The Contractor shall replace relieved Contractor personnel within 30 days of formal notification that Contractor personnel are “barred from post”. The Contractor remains

responsible for ensuring that all required positions are filled, as required. A manpower shortage that occurs due to misconduct on the part of Contractor personnel, or the receipt of unfavorable information concerning Contractor personnel that results in an individual being barred from post, shall be considered the responsibility of the Contractor to mitigate.

16.11 DATA RIGHTS

The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, produced and explicitly reimbursed for development under this contract shall be exclusively Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose.

This right does not abrogate any other Government rights.

16.12 PHYSICAL SECURITY

The Contractor shall be responsible for safeguarding all Government equipment, information and property provided to the Contractor. At the close of each work period, Government facilities, equipment, and materials shall be secured.

16.13 PERSONNEL SECURITY REQUIREMENTS

Access to classified documents, studies, reports, and other documentation and information may be required. Consequently, the contractor is required to provide personnel with U.S. security clearances, as required for mission execution upon contract award. When required, the contractor may be tasked to access a Sensitive unclassified network, and the duties to be performed by contractor personnel under the PWS have been designated as IT-I/IT-II sensitive positions. The contractor shall provide personnel with the appropriate level of security clearance background investigation and required security clearance at the time of award. Information gathered, developed, analyzed, and produced under this PWS remains the property of the US Army and shall be protected from unauthorized or inadvertent modification, disclosure, destruction, or use. Prior to the arrival of any contractor employee to commence work under this contract at any Government site, the contractor must provide advance notice to the Government for visitor control purposes and verification of security clearance.

DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce

Management requires active duty military, DoD civilian, DoD consultants, and support contractor personnel performing work on sensitive automated information systems (AISs) to be assigned to positions which are designated at one of three sensitivity levels (IAT – I, IAT – II, or IAT – III). These designations equate to Critical Sensitive and Non-Critical Sensitive positions. The employing contractor shall ensure individuals assigned to these sensitive positions have completed the appropriate access request forms. The Contractor personnel must be fully compliant with AR 25.8 and DoD 8570.1 training and certification prior to charging their costs to the contract.

IAT Level – I: Individuals assigned to positions where damage to DoD networks and development systems can be accomplished and no checks are in place to determine potential destruction of sensitive information. The investigation requirement for these positions is completion of a Special Security Background Investigation (SSBI) with favorable results.

IAT Level – II and III: Individuals assigned to positions where daily unsupervised access to DoD networks and information systems containing Sensitive but Unclassified or Sensitive Classified up to and including Collateral Secret information is a portion of their duties.

The investigation requirement for IAT Level II is completion of a National Agency Check with Local Agency and Credit Checks (NACLC) with favorable results. The investigation requirement for IAT Level III is a completion of a National Agency Check with Written Inquiries (NACI) with favorable results. (Note: For United States citizens, a submitted NACLC with a successful local records check will allow assignment to positions at the discretion of the Contracting Officer and in the best interest of the DoD before the completion of the investigation).

In all cases, the Contractor shall forward employee investigation information to the Contracting Officer before assignment of these individuals on this contract and shall ensure a visit request with that investigation information is provided yearly. Army Regulation (AR) 25-2 provides further information regarding the investigative requirements. The Government retains the right to request removal of contractor personnel, regardless of prior clearance or adjudication status, whose actions while assigned to this contract conflict with the interests of the Government. The reason for removal shall be fully documented in writing by the Contracting Officer.

16.14 POST AWARD CONFERENCE/PERIODIC PROGRESS MEETINGS

The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal

Acquisition Regulation Subpart 42.5. The Contracting Officer, COR, and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings, the contracting officer will apprise the contractor of how the Government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues.

The Contractor shall attend and support PdM I3MP monthly Project Status Review (PSR) meetings and other coordination meetings, as required. PdM I3MP will provide and arrange for meeting spaces within its facilities at Ft Belvoir for all required meetings with the Contractor. The Program Executive Officer – Enterprise Information Systems (PEO-EIS) dress code while on-site at Ft Belvoir is business-like and professional.

These meetings shall be at no additional cost to the Government.

16.15 ORGANIZATIONAL CONFLICT OF INTEREST

Contractor and Subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor’s mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.